8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,606	07/26/2001	Chengi Jimmy Kuo	NAI1P019/01.096.01	8718

28875 7590 03/23/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/916,606	**Applicant(s)** KUO, CHENGI JIMMY	
	Examiner Kevin Schubert	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 28 January 2005.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9,10,14-31,33,34 and 38-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9,10,14-31,33,34 and 38-55* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 28 January 2005 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

Claims 1-7,9,10,14-31,33,34, and 38-55 have been considered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7,9-10,14-18,24,26-31,33-34,38-42,44,50, and 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik, U.S. Patent No. 6,775,780, in view of Bowlin, U.S. Patent Application Publication No. 2002/0099944.

As per claims 1,24, and 50, the applicant describes a method for protecting a computer in an opened share mode comprising the following limitations which are met by Muttik in view of Bowlin:

a) running a computer on a network in an opened share mode, wherein the opened share mode indicates a file structure parameter and a name parameter and applies only to a manually selected list of at least one of application programs and data (Muttik: Col 3, lines 30-42; Fig 1; Bowlin: [0038]; Fig 6);

b) monitoring attempts to access the computer by applications utilizing the network, using the file structure and name parameter (Muttik: Col 1, lines 66-67; Col 2, lines 1-11; Fig 1; Bowlin: [0026]);

c) determining whether the applications attempt to modify the computer (Muttik: Col 2, lines 9-11; Fig 2);

d) executing a security event in response to any attempt to modify the computer (Muttik: Col 2, lines 12-15; Col 2, lines 31-36; Fig 2);

The applicant has not contested that the original limitations of the claim are met by Muttik. Muttik, however, does not disclose the amendment to the claim which includes the use of a file structure and name parameter for allowing a user to manually select which application programs are in opened share mode.

Bowlin discloses a method for protecting a computer in an opened share mode by allowing a user to manually select which application programs are in the opened share mode and which are in a virtual opened share mode where the application programs think they can access certain files but are actually barred from certain files if the user has not granted them access. The applicant should compare Fig 6 of Bowlin with Fig 6 of the applicant for the similarities between the two systems. Combining the ideas of Bowlin with Muttik would be simple. Instead of funneling every application through the virtual opened share mode as in Muttik, applications would be tested against the manually selected list of applications in the opened share mode to see which applications are in the opened share mode and which are in the virtual opened share mode.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Bowlin with those of Muttik because adding the use of selecting files based on file structure and name parameters lets a user designate which files he wants to be in the opened share mode and which he wants to be in the virtual opened share mode.

As per claims 2 and 26, the applicant discloses the method of claims 1 and 24, which are met by Muttik in view of Bowlin (see above), with the following limitation which is also met by Muttik:

Wherein the opened share mode allows other computers on the network to access data stored on the computer (Muttik: Col 3, lines 30-42);

As per claims 3 and 27, the applicant discloses the method of claims 1 and 24, which are met by Muttik in view of Bowlin (see above), with the following limitation which is also met by Muttik:

Wherein the opened share mode includes a virtual opened share mode (Muttik: Col 2, lines 2-5; Fig 2);

As can be seen by the lines referenced above and throughout the primary reference, the applications coming off the network are put in a virtual mode through the use of the emulator. Also, the applications have no knowledge they will be put through an emulator.

As per claims 4 and 28, the applicant discloses the method of claims 3 and 27, which are met by Muttik in view of Bowlin (see above), with the following limitation which is also met by Muttik:

Wherein the virtual opened share mode indicates to other computers of an ability to write to the computer (Muttik: Col 2, lines 2-5; Col 5, lines 10-11);

The applications coming from the network are placed in an insulated environment to monitor their system calls for malicious behavior (Col 2, lines 2-5). Furthermore, one system call that may be deemed malicious behavior is a system call to write an executable file with a particular name (Col 5, lines 10-11).

As per claims 5 and 29, the applicant discloses the method of claims 4 and 28, which are met by Muttik in view of Bowlin (see above), with the following limitation which is also met by Bowlin:

Wherein the computer operates in the virtual opened share mode by modifying an application program interface (Bowlin: [0035]; [0044]);

The computer modifies an application program interface by associating it with a filter to see if the requested file is within the safe zone.

As per claims 6 and 30, the applicant describes the method of claims 5 and 29, which are met by Muttik in view of Bowlin (see above), with the following limitation which is met by Bowlin:

Wherein the application program interface includes an operating system application program interface (Bowlin: [0035]);

As per claims 7 and 31, the applicant describes the method of claims 5 and 29, which are met by Muttik in view of Bowlin (see above), with the following limitation which is met by Bowlin:

Wherein the application program interface includes a network application program interface (Bowlin: [0035]);

Bowlin discloses an application program interface which is used to interface with network applications.

As per claims 9 and 33, the applicant describes the method of claims 1 and 24, which are met by Muttik in view of Bowlin (see above), with the following limitation which is met by Bowlin:

Wherein the opened share mode indicates a plurality of parameters that are randomly selected to prevent detection (Bowlin: [0038]);

Bowlin describes a system where the user randomly selects the parameters which are incorporated as being in the open share mode.

As per claims 10 and 34, the applicant discloses the method of claims 1 and 24, which are met by Muttik in view of Bowlin (see above), with the following limitation which is also met by Muttik:

Wherein the opened share mode applies to each of a plurality of networks of which the computer is a member (Muttik: Col 3, lines 37-42; Fig 1);

The applicant should note the network (102 in Fig 1) can include a “combination of networks” (Col 3, lines 40-41).

As per claims 14 and 38, the applicant describes the method of claims 1 and 24, which are met by Muttik in view of Bowlin (see above), with the following limitation which is met by Bowlin:

Wherein the computer is run on the network in a plurality of opened share modes (Bowlin: [0044]);

A plurality of opened share modes is created because different users have different access levels to applications.

As per claims 15 and 39, the applicant discloses the method of claims 1 and 24 respectively, which are met by Muttik in view of Bowlin (see above), with the following limitation which is also met by Muttik:

Wherein any attempt to modify the computer is utilized in a heuristic analysis for identifying a coordinated attack on multiple computers (Muttik: Col 1, lines 66-67; Col 2, lines 1-11);

The applicant should note that the emulator records a pattern of system calls and analyzes the behavior of the application which can be viral in a heuristic analysis type approach. The rules (210 of Fig 2) can be set to a plurality of preferences, including determination of a coordinated attack.

As per claims 16 and 40, the applicant discloses the method of claims 1 and 24 respectively, which are met by Muttik in view of Bowlin (see above), with the following limitation which is also met by Muttik:

Wherein attempts to modify the computer are tracked (Muttik: Col 3, lines 66-67; Col 4, lines 1-11; Fig 2);

As illustrated in Fig 2 and the lines referenced above, system calls are tracked and then fed into a comparator for determination of malicious behavior.

As per claims 17-18 and 41-42, the applicant discloses the method of claims 1 and 24 respectively, which are met by Muttik in view of Bowlin (see above), with the following limitation which is also met by Muttik:

Wherein it is determined whether the applications attempt to write to memory in the computer, and the security event is executed in response to any attempt to write to memory in the computer (Muttik: Col 5, lines 10-11);

As described above, attempting to write a file with a particular name to memory is one example of a rule that can be set to determine malicious behavior. If the user desires, any attempt to write to memory could be deemed malicious behavior. Regarding claims 18 and 42, this includes any attempt to copy the virus to memory. Also, the security event can be alerting the user (Col 2, lines 12-15) or terminating analysis of the software thereby not allowing the software or application to be executed in real space (Col 2, lines 31-36). The use of either of these security events or both of these security events depends on which embodiment of the primary reference is used.

As per claims 20 and 44, the applicant discloses the method of claims 1 and 24 respectively, which are met by Muttik in view of Bowlin (see above), with the following limitation which is also met by Muttik:

Wherein the security event includes terminating the application attempting to modify the computer (Muttik: Col 2, lines 31-36);

As described earlier, terminating the analysis of the software attempting to modify the computer based on a decision that the software is malicious means that the software will not be executed in real time since software coming off the network must pass the emulator test before being executed in real time.

As per claim 25, the applicant discloses the method of claim 24, which is met by Muttik in view of Bowlin (see above), with the following limitation which is also met by Muttik:

Wherein the network includes the Internet (Muttik: Col 3, lines 19-21).

As per claim 53, the applicant describes the method of claim 1, which is met by Muttik in view of Bowlin (see above), with the following limitation which is met by Bowlin:

Wherein the file structure includes a tree structure (Bowlin: Fig 6).

As per claim 54, the applicant describes the method of claim 1, which is met by Muttik in view of Bowlin (see above), with the following limitation which is met by Bowlin:

Wherein the computer is run in an actual opened share mode and a virtual opened share mode such that the at least one of application programs and data is accessible in the actual opened share mode, and attempted access to the at least one of application programs and data associated with the virtual opened shared mode prompts a security process (Bowlin: [0026]).

Claims 19,21-23,43,45-47,51, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik in view of Bowlin in further view of Schnurer, U.S. Patent No. 5,842,002.

As per claims 19 and 43, the applicant describes the method of claims 1 and 24, which are met by Muttik in view of Bowlin (see above), with the following limitation which is met by Schnurer:

Wherein the security event includes logging the computer off the network in response to any attempt to modify the computer (Schnurer: Col 8, lines 26-35);

Muttik in view of Bowlin discloses all the limitations of the independent claims. However, Muttik in view of Bowlin fails to go into detail about the actions taken when malicious code is detected. Schnurer discloses a virus trap system similar to Muttik's and Bowlin's in which certain actions are taken when malicious code is detected. One of these actions is "shutting down a network segment" (Col 8, line 33). This includes logging a computer off the network. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schnurer with those of Muttik in view of Bowlin to further protect the computer once an application has been deemed malicious.

As per claims 21 and 45, the applicant describes the method of claims 1 and 24, which are met by Muttik in view of Bowlin (see above), with the following limitation which is met by Schnurer:

Wherein the security event includes deleting the application attempting to modify the computer (Schnurer: Col 8, lines 26-35);

As per claims 22 and 46, the applicant describes the method of claims 1 and 24, which are met by Muttik in view of Bowlin (see above), with the following limitation which is met by Schnurer:

Wherein the security event includes an alert transmitted via the network (Col 8, lines 26-35);

As per claims 23 and 47, the applicant describes the method of claims 22 and 46, which are met by Muttik in view of Bowlin in further view of Schnurer (see above), with the following limitation which is met by Schnurer:

Wherein the security event includes information associated with the application attempting to modify the computer (Col 8, lines 26-35);

As per claims 51 and 52, the applicant describes a method for protecting a computer in an opened share mode comprising the following limitations which are met by Muttik in view of Bowlin in further view of Schnurer:

a) running a computer on a network in a virtual opened share mode and an actual opened share mode, wherein the virtual opened share mode allows other computers on the network to access predetermined data and programs resident on the computer, and indicates to other computers of an ability to write to the computer, and the actual opened share mode indicates a file structure parameter and a name parameter that are capable of actually being accessed by the other computers, and applies only to a manually selected list of at least one of application programs and data (Muttik: Col 3, lines 30-42; Fig 1; Bowlin: [0038]; Fig 6);

b) monitoring attempts to access the computer by applications utilizing the network, using, at least in part, the file structure and name parameter (Muttik: Col 1, lines 66-67; Col 2, lines 1-11; Fig 1; Bowlin: [0026]);

c) determining whether the applications attempt to modify the computer (Muttik: Col 2, lines 9-11; Fig 2);

d) tracking the attempts of the applications to modify the computer (Muttik: Col 3, lines 66-67; Col 4, lines 1-11; Fig 2);

e) transmitting an alert via the network in response to any attempt to modify the computer, wherein the alert includes information associated with the applications attempting to modify the computer (Schnurer: Col 8, lines 26-35);

f) logging the computer off the network in response to any attempt to modify the computer (Schnurer: Col 8, lines 26-35);

g) deleting any application attempting to modify the computer (Schunurer: Col 8, lines 26-35);

h) wherein any attempt to modify the computer is utilized in a heuristic analysis for identifying a coordinated attack on multiple computers (Muttik: Col 1, lines 66-67, Col 2, lines 1-11);

i) wherein (d)-(h) are carried out if it is determined that the applications attempt to modify the computer via the virtual opened share mode; and access is permitted if it is determined that the applications attempt to modify the computer via the actual opened share mode (Bowlin: [0026]; Schnurer: Col 8, lines 26-35);

As described in the rejection for claim 1, Muttik in view of Bowlin discloses a system which incorporates an actual opened share mode (through manually selected files based on their file structure and name parameters) and a virtual opened share mode where a network application accesses a computer thinking he has the ability to write to a particular file but is actually barred from access to the particular file if the user has not designated him having access by manually selected the file for the opened share mode.

Muttik in view of Bowlin, however, fail to go into detail about the actions taken when malicious code is detected. Schnurer discloses a virus trap system similar to Muttik's and Bowlin's in which certain actions are taken when malicious code is detected. These actions include transmitting an alert, deleting an application, and logging a computer off the network (Schnurer: Col 8, lines 26-35). Incorporating the ideas of Schnurer into the system of Muttik in view of Bowlin would simply mean that Schnurer's ideas for dealing with malicious code are executed when an application attempts to modify a file that it is not supposed to (ie, a file which is not on the manually selected opened share list).

It would have been obvious to one of ordinary skill in the art to combine the ideas of Schnurer with those of Muttik in view of Bowlin because Schnurer discloses actions that can be taken once malicious code has been detected to prevent the malicious code from doing damage to the system.

Claims 48 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik in view of Bowlin in further view of Jordan, U.S. Patent Application Publication No. 2002/0073323.

As per claims 48 and 49, the applicant limits the computer program product of claim 24, which is met by Muttik in view of Bowlin (see above), with the following limitation which is met by Jordan:

Wherein at least a portion of the computer code resides on a gateway (Jordan: [0029] and [0030]);

Muttik discloses all the limitations of the independent claim. However, Muttik fails to disclose the use of a gateway. Jordan describes a similar virus protection system to Muttik's in which applications are put in a virtual space before being actually run on a computer.

Jordan also describes having the apparatus and methods of the system be embodied in a transmission medium [0029]. Jordan further discloses that "the computer virus detection methodologies may be performed on a file... before the file is stored/copied/executed/opened on the computer" [0030]. A gateway is a transmission medium which connects the user to the network. Though Jordan does not explicitly use the term gateway, he does disclose the idea of using a gateway or similar device to analyze the application before it goes to the computer. Regarding claim 49 and in accordance with both Muttik and Jordan, if the file is determined to be malicious it would therefore be blocked from entering the computer. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Muttik with those of Jordan and implement the use of a gateway to block access to a computer so that files are analyzed and discarded before they even have a chance to get to the computer.

Claim 55 is rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik in view of Bowlin in further view of Schnurer in further view of Porras, U.S. Patent No. 6,704,874.

As per claim 55, the applicant describes the method of claim 54, which is met by Muttik in view of Bowlin (see above), with the following limitation which is met by Muttik in view of Schnurer in further view of Porras:

a) wherein the security process includes temporarily logging off the network (Schnurer: Col 8, lines 26-35);

b) recording in a record information on any attempt to modify the computer including time and source information (Muttik: Col 4, lines 32-44);

c) logging the computer back on the network in a mode other than the actual opened share mode (Muttik: Abstract, Fig 1);

d) transmitting the information to a third party (Porras: Col 2, lines 12-37; Col 8, lines 52-61)

e) determining whether a trend is found indicative of a coordinated attack (Porras: Col 2, lines 12-37; Col 8, lines 26-35);

f) sending an alert and logging a culpable computer off the network based on the determination (Schnurer: Col 8, lines 26-35);

Muttik in view of Bowlin discloses all the limitations of claim 54. Muttik in view of Bowlin, does not disclose the exact security process described above. Muttik does disclose the idea of recording information of attempts to modify the computer by recording chronological attempts of particular sources or applications (part b). Also, Muttik discloses the idea of a computer logging on a network and functioning in a virtual opened share mode, which is a mode other than the actual opened share mode (part c). Muttik in view of Bowlin, however, does not disclose parts a) and d) through f).

Schnurer discloses how a computer virus trap system deals with malicious code when it finds malicious code. Among the features described by Schnurer are sending an alert and logging a culpable computer off the network (parts a) and f)). Combining the ideas of Schnurer with those of Muttik in view of Bowlin would be easy because Muttik in view of Bowlin disclose how to catch malicious code and Schnurer simply discloses what to do with the malicious code when it is caught. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of

Schnurer with those of Muttik in view of Bowlin because doing so would allow the system to effectively deal with malicious code when it is identified.

Muttik in view of Bowlin in further view of Schnurer fails to describe parts d) and e) in which a third party analyzes information for a trend indicative of a coordinated attack. Porras discloses this feature in which an alert manager third party analyzes received information to determine whether a coordinated attack is taking place. Including the ideas of Porras into the system of Muttik in view of Bowlin in further view of Schnurer would simply require the addition of the third party alert manager system which is used to determine whether a coordinated attack is taking place. When the determination from the alert manager comes back, then the security features described by Schnurer such as sending an alert to an administrator and/or logging a culpable computer off the network would take place. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Porras with those of Muttik in view of Bowlin in further view of Schnurer because having a third party test for a coordinated attack provides enhanced security.

Response to Arguments

Applicant's arguments, see Remarks, filed 1/28/05, with respect to the rejection(s)of claim(s) 8 and 11-12 under Muttik in view of Jordan have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Bowlin, U.S. Patent Application Publication No. 2002/0099944.

Applicant's arguments with respect to the rejection(s)of claim(s) 5 under Muttik have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Bowlin, U.S. Patent Application Publication No. 2002/0099944.

Applicant's arguments with respect to the rejection(s)of claim(s) 9 under Muttik have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Bowlin, U.S. Patent Application Publication No. 2002/0099944.

Applicant's arguments with respect to the rejection(s)of claim(s) 6 and 7 under Muttik have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Bowlin, U.S. Patent Application Publication No. 2002/0099944.

Applicant's arguments with respect to the rejection(s)of claim(s) 48 have been fully considered but they are not persuasive. Though Jordan does not explicitly use the word gateway, he does disclose the ideas of a gateway device which provides functionality to block a malicious application before it even gets to the computer.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER